

**Homeland
Security**

Operation Flicker ICE – Special Training Notice 2013

The Department of Homeland Security (DHS) has released a training notice for the Immigration and Customs Enforcement (ICE) –OF Modernization program. This training notice represents the program's domestic operations for law enforcement to be effective against the sexual exploitation of children which includes child pornography.

Description and Background:

Past methods used to combat and fight child pornography distribution and possession were not very effective as many have resorted to clever and sophisticated methods to avoid detection by internet monitoring systems set up online with help of the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). As of 2011 to 2013, new methods have been adopted for the current law enforcement system supporting the screening of peer-to-peer file sharing networks and other internet protocols for detecting child pornography distribution and downloading.

Programmatically, ICE Operation Flicker is limited in detecting and aiding in catching child pornographers as they continue finding sophisticated methods to avoid detection from law enforcement. So this short special training notice has given notice of instructing new methods, tactics, and strategies in order to train ICE and federal law enforcement to catch potential child pornographers whom have been caught engaging in sex tourism and exploitation of children. These methods involve both P2P file sharing systems and using computer Trojans which can be distributed on both encrypted and non-encrypted networks. These methods ensure that law enforcement has the proper tools that can finally catch child molesters and child exploiters whom have avoided child porn detection schemes by undercover agents and officers.

Risks and Issues:

The use of these methods may create constitutional and legal issues which may drive radical civil liberties organizations to attempt to fight these new methods upon discovery of them, which is the reason why this document remains classified, however the benefits of fighting sex tourism and child exploitation make these new methods acceptable in the modern age of telecommunications. The few risks in addition to the above are identified below:

- If ICE and FBI are not coordinated in their attempts using these new methods to deter and catch potential child pornographers, there may be data consistency issues between the agencies and data leaks from potential whistleblowers.
- Child pornography files may have to be shared from CPS servers in order to execute these new methods which will help criminal investigators determine if whom they are investigating could engage in distribution and transmission of child pornography images and moving images.
- The new methods of using Trojans and P2P file sharing systems to engage potential child pornographers to download files from undercover agents will prove more of a success since tools now exist to block and blacklist government IP Addresses which further deters our agents from being able to detect those engaging in distribution and transmission.

Trojan Strategy:

The Trojans shall be developed by our IT technicians and programming teams coordinated between the FBI Cyber Crime division and ICE. The purpose of these programs is to infect anyone whom is added to our suspected child-pornographer lists then use them to download child pornography then distribute them with other users on P2P file sharing networks to be able to flag the IP Address then sent it to the National Center for Missing and Exploited Children (NCMEC). The Trojans will use the following procedures to engage in the catching of suspects.

- ICE will work closely with the FBI to develop Trojans that specifically can patch into all standard P2P protocols including ed2k, gnutella, Kad, Bittorrent, and any other similar protocols concerning the distribution and trading of files.
- The Trojans used will be mainly Windows based and will be difficult to end the task and remove using a task manager or any conventional methods of process termination. The Trojans will store the child pornography in folders of which the average user is not aware of or has no expertise of. The files shared will be files which were already flagged by the NCMEC for this method to be effective.

P2P file sharing strategy:

ICE's new method to catch child predators using P2P file sharing software is by sharing files which will not be found under the suspects radar. Sharing files using terms such as PTHC, PTSC, R@ygold, hussyfan, 12yo, 11yo, etc. and other terms has proven more difficult as pedophiles have become aware of the sting operations using these keywords. This method has been adopted and has been used for already two years and has so far had success with gaining approval after submitting key documents of these procedures. The procedure will be using the new methods which include stuffing child pornography images and moving-images inside of average files which will be shared by servers sanctioned by the FBI. The methods of stuffing will vary from each agent or officer but are approved as long as the suspect cannot detect that the file contains child pornography until the file has been downloaded. Child pornography has successfully been stuffed into adult pornography films, music files using ID3 tags, software programs, keygens and cracks, and other material that has been illicitly traded over P2P file sharing networks. This method has been successful at deterring both child pornographers and copyright infringement and has been approved for official procedures under the guise that it be kept as classified information. Stuffing has prevented child pornographers from being able to avoid our detection systems and have been used to finally net difficult child pornography distributors and downloaders.

Score: 4